REMARKS

Assignee respectfully requests entry of the following amendments and remarks in response to the Final Office Action mailed November 23, 2009. Assignee respectfully submits that the amendments and remarks contained herein place the instant application in condition for allowance.

Upon entry of the amendments in this response, claims 1, 6, 11 – 14, 16, 17, and 19 – 40 are pending. In particular, Assignee adds claim 40 and amends claims 1, 6, 11 – 14, 16, 17, and 19 – 39. Reconsideration and allowance of the application and presently pending claims are respectfully requested.

I. Claim Objections

The Office Action objects to claims 23 – 25 and 30 – 32 for various informalities. Assignee amends claims 23 – 25 and 30 – 32, as indicated above, and submits that these amendments overcome this objection.

II. Objections to the Specification

The Office Action indicates that the specification is objected to as failing to provide proper antecedent basis for the subject matter of claim 6. Assignee respectfully traverses this rejection. More specifically, MPEP §608.01(o) states:

> [u]sually the terminology of the original claims follows the nomenclature of the specification, but sometimes in amending the claims or in adding new claims, new terms are introduced that do not appear in the specification…
> (Emphasis added).

Assignee submits that, as illustrated in the passage above, the MPEP provides for scenarios where terms do not appear in the specification. However, as long as one of ordinary

skill in the art would understand the scope of the specification to include the claimed subject matter, 35 U.S.C. §112 is fulfilled.

With regard to claim 6, each of the terms would unquestionably be understood by one of ordinary skill in the art as being a concept included in the specification of the present application. As a nonlimiting example, the Specification discloses the fact that an SMTP address may indicate "a sender's email address, a reply-to address, or other recipients that are carbon-copied (cc'd) on the email message" (page 6, line 1). One would unquestionably understand (from at least this passage) that an SMTP address would include displaying characters (*e.g.*, characters that are being displayed). For at least this reason, Assignee respectfully traverses this objection.

III. Rejections Under 35 U.S.C. §112, Second Paragraph

The Office Action rejects claims 1, 6, and 39 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Assignee regards as the invention. Assignee respectfully traverses this rejection for at least the reason that the claims are clear on their face and are fully supported in at least FIGS. 8A and 8B, beginning page 18, line 21, as well as elsewhere. More specifically, as illustrated in this passage, the process of determining whether there is a solitary 'i' or 'a' relates to the removal of non-alphabetic characters to facilitate tokenizing at least a portion of the email message. Consequently, Assignee submits that there is no confusion and that claims 1 and 39 meet all the requirements of 35 U.S.C. §112.

Further, with regard to claim 6, as indicated above, "the displaying characters of the SMTP email address" refers to characters of the SMTP email address that are being displayed. As also previously indicated, this element is clearly disclosed in the Specification. For at least this reason, claim 6 meets all the requirements of 35 U.S.C. §112.

IV. Rejections Under 35 U.S.C. §103

A. Claim 6 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 6 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 6. More specifically, claim 6 recites:

> A method comprising:
> receiving, at a computing device, ~~an~~ a first email message comprising a text body, an SMTP email address, an attachment, and a domain name corresponding to the SMTP email address, the text body including displaying characters and non-displaying characters;
> searching for the non-displaying characters in the first email message;
> removing the searched non-displaying characters, including non-displaying comments and non-displaying control characters;
> tokenizing the SMTP email address to generate an address token representative of the displaying characters of the SMTP email address;
> tokenizing the attachment to generate an attachment token that is representative of the attachment;
> tokenizing the domain name to generate a domain token representative of the domain name;
> determining a corresponding spam probability value from the address token, the attachment token, and the domain token;
> ***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens:***
> ***updating the spam probability value of at least one of the address token, the attachment token, and the domain token;***
> ***sorting the address token, the attachment***

> ***token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token***; and
> ***filtering a second email message.***
> ***(Emphasis added).***

Claim 1, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek* "***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… updating the spam probability value of at least one of the address token, the attachment token, and the domain token… sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token…*** [and] ***filtering a second email message***" as recited in claim 1, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests "***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… updating the spam probability value of at least one of the address token, the attachment token, and the***

domain token*... *sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token*...** [and] ***filtering a second email message" as recited in claim 1, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest "***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens*... *updating the spam probability value of at least one of the address token, the attachment token, and the domain token*... *sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token*...** [and] ***filtering a second email message***" as recited in claim 1, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)... [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than "***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination***

that at least one of the address token, the attachment token, and the domain token is present in the database of tokens... updating the spam probability value of at least one of the address token, the attachment token, and the domain token... sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token... [and] ***filtering a second email message***" as recited in claim 1, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than "***determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens... updating the spam probability value of at least one of the address token, the attachment token, and the domain token... sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token...*** [and] ***filtering a second email message***" as recited in claim 1, as amended. For at least these reasons, claim 1, as amended, is allowable.

B. Claim 23 is Allowable Over *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*

The Office Action indicates that claim 23 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 23. More specifically, claim 23 recites:

> A system comprising:
> a memory component that stores at least the following:
> email receive logic configured to receive ~~an~~ a first email message comprising an SMTP email address, a domain name corresponding to the SMTP email address, and an attachment, the first email message further including displaying characters and non-displaying characters;
> searching logic configured to search for the non-displaying characters in the first email message;
> removing logic configured to remove the non-displaying characters, including non-displaying comments and non-displaying control characters;
> tokenize logic configured to tokenize the SMTP email address to generate an address token representative of the SMTP email address;
> tokenize logic configured to tokenize the attachment to generate an attachment token that is representative of the attachment;
> tokenize logic configured to tokenize the domain name to generate a domain token representative of the domain name;
> analysis logic configured to determine a corresponding spam probability value from the address token, the attachment token, and the domain token; and
> ***determine logic configured to determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens***:
> ***update the corresponding spam probability value of the address token, the attachment token, and the domain token***;
> ***sort the address token, the attachment token, and the domain token in accordance with the corresponding***

spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized; and

filter a second email message.

(Emphasis added).

Claim 23, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "system comprising… a memory component that stores at least the following… ***determine logic configured to determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and the domain token… sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 23, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests "a memory component that stores at least the following… ***determine logic configured to determine whether at least one of the address token, the attachment token, and the***

domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens... update the corresponding spam probability value of the address token, the attachment token, and the domain token... sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized... [and] ***filter a second email message***" as recited in claim 23, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest "a memory component that stores at least the following... ***determine logic configured to determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens... update the corresponding spam probability value of the address token, the attachment token, and the domain token... sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized...*** [and] ***filter a second email message***" as recited in claim 23, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)… [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than "a memory component that stores at least the following… ***determine logic configured to determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and the domain token… sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 23, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than "a memory component that stores at least the following… ***determine logic configured to determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and***

***the domain token*... *sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized*... [and] *filter a second email message*"** as recited in claim 23, as amended. For at least these reasons, claim 23, as amended, is allowable.

C. Claim 24 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 24 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 24. More specifically, claim 24 recites:

> A system comprising:
> means for receiving a first email message comprising an SMTP email address, a domain name corresponding to the SMTP email address, and an attachment, the first email message further including displaying characters and non-displaying characters;
> means for searching for the non-displaying characters in the first email message;
> means for removing the non-displaying characters, including non-displaying comments and non-displaying control characters;
> means for tokenizing the SMTP email address to generate an address token representative of the SMTP email address;
> means for tokenizing the attachment to generate an attachment token that is representative of the attachment;
> means for tokenizing the domain name to generate a domain token representative of the domain name;
> means for determining a corresponding spam probability value from the address token, the attachment token, and the domain token;

means for determining whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens; and

means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens:

updating the spam probability value of the address token, the attachment token, and the domain token;

sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized; and

filtering a second email message.

(Emphasis added).

Claim 24, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "system comprising… ***means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… updating the spam probability value of the address token, the attachment token, and the domain token… sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized…*** [and] ***filtering a second email message***" as recited in claim 24, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that

even suggests "***means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens*... *updating the spam probability value of the address token, the attachment token, and the domain token*... *sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized***... [and] ***filtering a second email message***" as recited in claim 24, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest "***means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens*... *updating the spam probability value of the address token, the attachment token, and the domain token*... *sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized***... [and] ***filtering a second email message***" as recited in claim 24, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)... [is] also [a] powerful distinguisher between junk and

legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than "***means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… updating the spam probability value of the address token, the attachment token, and the domain token… sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized…*** [and] ***filtering a second email message***" as recited in claim 24, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than "***means for, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… updating the spam probability value of the address token, the attachment token, and the domain token… sorting the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the address token, the attachment token, and the domain token, wherein only displaying characters are tokenized…*** [and] ***filtering a second email message***" as recited in claim 24, as amended. For at least these reasons, claim 24, as amended, is allowable.

D. Claim 25 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 25 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 25. More specifically, claim 25 recites:

> A computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following:
> receive ~~an~~ a first email message comprising an SMTP email address, a domain name corresponding to the SMTP email address, and an attachment, the first email message further including displaying characters and non-displaying characters;
> search for non-displaying characters in the first email message;
> remove the non-displaying characters, including non-displaying comments and non-displaying control characters;
> tokenize the SMTP email address to generate an address token representative of the SMTP email address;
> tokenize the attachment to generate an attachment token that is representative of the attachment;
> tokenize the domain name to generate a domain token representative of the domain name;
> determine a corresponding spam probability value from the address token, the attachment token, and the domain token; and
> ***determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens***:
> ***update the corresponding spam probability value of the address token, the attachment token, and the domain token***;
> ***sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***; and

filter a second email message.
(Emphasis added).

Claim 25, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and the domain token… sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***… [and] ***filter a second email message***" as recited in claim 25, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the***

domain token is present in the database of tokens*... *update the corresponding spam probability value of the address token, the attachment token, and the domain token*... *sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized*...** [and] ***filter a second email message" as recited in claim 25, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following... ***determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens*... *update the corresponding spam probability value of the address token, the attachment token, and the domain token*... *sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized*...** [and] ***filter a second email message***" as recited in claim 25, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most

junk E-mail does not have them)… [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following***… determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and the domain token… sort the address token, the attachment token, and the domain token in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 25, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether at least one of the address token, the attachment token, and the domain token is present in a database of tokens and, in response to a determination that at least one of the address token, the attachment token, and the domain token is present in the database of tokens… update the corresponding spam probability value of the address token, the attachment token, and the domain token… sort the address token, the attachment token, and the domain token in accordance with the corresponding spam***

probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized... [and] ***filter a second email message***" as recited in claim 25, as amended. For at least these reasons, claim 25, as amended, is allowable.

E. Claim 30 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 30 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 30. More specifically, claim 30 recites:

> A system comprising:
> a memory component that stores at least the following:
> email receive logic configured to receive a first email message comprising an attachment and an address, the email message further including displaying characters and non-displaying characters;
> search logic configured to search for the non-displaying characters in the first email message;
> remove logic configured to remove the non-displaying characters, including non-displaying comments and non-displaying control characters;
> tokenize logic configured to generate at least one attachment token representative of the attachment;
> analysis logic configured to determine a corresponding spam probability value from the at least one attachment token; and
> database determining logic configured to determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens:
> update the corresponding spam probability value of the at least one attachment token;
> sort the at least one attachment token in

> accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the at least one attachment token, wherein only displaying characters are tokenized; and
>
> filter a second email message.

(Emphasis added).

Claim 30, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "system comprising… a memory component that stores at least the following… ***database determining logic configured to determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the corresponding spam probability value of the at least one attachment token… sort the generated tokens in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 30, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests "***database determining logic configured to determine whether at least one of the tokens is present in the database of tokens and, in response to a determination that at least one of the tokens is present in the database of tokens… update the corresponding spam probability value of that at least one token… sort the generated tokens in accordance with the***

corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized... [and] ***filter a second email message***" as recited in claim 30, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest "***database determining logic configured to determine whether at least one of the tokens is present in the database of tokens and, in response to a determination that at least one of the tokens is present in the database of tokens... update the corresponding spam probability value of that at least one token... sort the generated tokens in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***... [and] ***filter a second email message***" as recited in claim 30, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)... [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than "***database determining logic configured to determine whether at least one of the tokens is present in the database of tokens and, in response to a determination that at least one of the tokens is present in the database of tokens... update the corresponding spam probability value of that at least one token... sort the generated tokens in***

accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized... [and] ***filter a second email message***" as recited in claim 30, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than "***database determining logic configured to determine whether at least one of the tokens is present in the database of tokens and, in response to a determination that at least one of the tokens is present in the database of tokens... update the corresponding spam probability value of that at least one token... sort the generated tokens in accordance with the corresponding spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***... [and] ***filter a second email message***" as recited in claim 30, as amended. For at least these reasons, claim 30, as amended, is allowable.

F. Claim 31 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 31 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that

Shipp in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 31. More specifically, claim 31 recites:

> A system comprising:
> means for receiving a first email message comprising an attachment and an address, the first email message further including displaying characters and non-displaying characters;
> means for searching for non-displaying characters in the first email message;
> means for removing the non-displaying characters, including non-displaying comments and non-displaying control characters;
> means for generating an at least one attachment token representative of the attachment;
> means for determining a spam probability value from the at least one attachment token;
> means for determining whether the at least one attachment token is present in a database of tokens; and
> ***means for, in response to a determination that the at least one attachment token is present in the database of tokens:***
> ***updating the spam probability value of the*** at ***least one attachment token***;
> ***sorting the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***; and
> ***filtering a second email message.***
> ***(Emphasis added).***

Claim 31, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "system comprising*... **means for, in response to a determination that the at least one attachment token is present in the database of tokens**... **updating the spam probability value of the at least one attachment token**... **sorting the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***... [and] ***filtering a second email message***" as recited in claim 31, as amended.

More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests "***means for, in response to a determination that the at least one attachment token is present in the database of tokens*... *updating the spam probability value of the at least one attachment token*... *sorting the attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized*... [and] *filtering a second email message***" as recited in claim 31, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages, including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest "***means for, in response to a determination that the at least one attachment token is present in the database of tokens*... *updating the spam probability value of the at least one attachment token*... *sorting the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized*... [and] *filtering a second email message***" as recited in claim 31, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)... [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than "***means for, in response to a determination that the at least one attachment token is present in the database of tokens... updating the spam probability value of the at least one attachment token... sorting the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized...*** [and] ***filtering a second email message***" as recited in claim 31, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than "***means for, in response to a determination that the at least one attachment token is present in the database of tokens... updating the spam probability value of the at least one attachment token... sorting the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized...*** [and] ***filtering a second email message***" as recited in claim 31, as amended. For at least these reasons, claim 31, as amended, is allowable.

G. Claim 32 is Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claim 32 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claim 32. More specifically, claim 32 recites:

> A computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following:
> receive a first email message comprising an attachment and an address, the first email message further including displaying characters and non-displaying characters;
> search for the non-displaying characters in the first email message;
> remove the non-displaying characters, including non-displaying comments and non-displaying control characters;
> generate an at least one attachment token representative of the attachment;
> determine a spam probability value from the at least one attachment token; and
> ***determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens:***
> ***update the spam probability value of the at least one attachment token***;
> ***sort the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized***; and
> ***filter a second email message***.
> ***(Emphasis added).***

Claim 32, as amended, is allowable over the cited art for at least the reason that none of *Shipp*, *Milliken*, *Sahami*, and *Woitaszek*, taken alone or in combination, discloses, teaches, or suggests a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether the at least one***

attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the spam probability value of the at least one attachment token… sort the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized… [and] ***filter a second email message***" as recited in claim 32, as amended. More specifically, *Shipp* discloses "[i]t is often possible to identify which application generated a particular email by examining the email headers and also [by] examining the format of the different parts. It is then possible to identify emails which contain quirks which either indicate that the email is attempting to look as if it was generated by a known emailer, but was not, or that it was generated by a new and unknown mailer, or by an application" (page 2, paragraph [0043]). However, there is nothing in *Shipp* that even suggests a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the spam probability value of the at least one attachment token… sort the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 32, as amended.

Similarly, *Milliken* fails to overcome the deficiencies of *Shipp*. More specifically, *Milliken* discloses "provid[ing] virus, worm, and unsolicited e-mail detection and/or prevention in email servers. Placing these features in e-mail servers provides a number of new advantages,

including the ability to align hash blocks to crucial boundaries found in e-mail messages" (page 2, paragraph [0024]). However, *Milliken* fails to suggest a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the spam probability value of the at least one attachment token… sort the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 32, as amended.

Further, *Sahami* fails to overcome the deficiencies of *Shipp* and *Milliken*. More specifically, *Sahami* discloses "[determining] whether a message has attached documents (most junk E-mail does not have them)… [is] also [a] powerful distinguisher between junk and legitimate E-mail" (page 3, right column, last paragraph). However, this is completely different than a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the spam probability value of the at least one attachment token… sort the at least one attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 32, as amended.

Additionally, *Woitaszek* fails to overcome the deficiencies of *Shipp*, *Milliken*, and *Sahami*. More specifically, *Woitaszek* discloses "[e]ach message [is] parsed to completely remove any headers, attachments, HTML markup, punctuation, and extended characters. This procedure essentially reduces a mail message to a series of delimited lowercase string tokens" (page 2, section 4). Again, this is different than a "computer-readable storage medium that includes a program that, when executed by a computer, performs at least the following… ***determine whether the at least one attachment token is present in a database of tokens and, in response to a determination that the at least one attachment token is present in the database of tokens… update the spam probability value of the at least one attachment token… sort the attachment token in accordance with the spam probability value to determine a predefined number of interesting tokens, the predefined number of interesting tokens being a subset of the generated tokens, wherein only displaying characters are tokenized…*** [and] ***filter a second email message***" as recited in claim 32, as amended. For at least these reasons, claim 32, as amended, is allowable.

H. Claims 11 – 14, 16, 17, 19 – 22, 26 – 29, and 33 – 38 are Allowable Over *Shipp, Milliken, Sahami,* and *Woitaszek*

The Office Action indicates that claims 11 – 14, 16, 17, 19 – 22, 26 – 29, and 33 – 38 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication Number 2004/0093384 ("*Shipp*") in view of U.S. Patent Publication Number 2004/0073617 ("*Milliken*"), A Bayesian Approach to Filtering Junk E-Mail ("*Sahami*") and Identifying Junk Electronic Mail In Microsoft Outlook with a Support Vector Machine ("*Woitaszek*"). This rejection is improper for at least the reason that *Shipp* in view of *Milliken, Sahami,* and *Woitaszek* fails to disclose, teach, or suggest all of the elements of claims 11 – 14, 16, 17, 19 – 22, 26 – 29, and 33 – 38. More specifically, dependent claims 11 – 14, 16, 17 and

19 – 22 are allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 1. Dependent claims 26 – 29 are allowable for at least the reason that these claims depend from and include the elements of allowable independent claim 25. Further, dependent claims 33 – 36 are allowable for at least the reason that they depend from and include the elements of allowable independent claim 32. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002).

V. New Claim 39

In addition, Assignee adds new claim 39. New claim 39 is allowable over the cited art for at least the reason that this claim depends from allowable independent claim 1. *In re Fine*, *Minnesota Mining and Mfg.Co. v. Chemque, Inc.*, 303 F.3d 1294, 1299 (Fed. Cir. 2002). Support for this claim may be found, among other places, on page 18, line 21.

CONCLUSION

In light of the foregoing amendments and for at least the reasons set forth above, all objections and/or rejections have been traversed, rendered moot, and/or addressed, and that the now pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested.

Any other statements in the Office Action that are not explicitly addressed herein are not intended to be admitted. In addition, any and all findings of inherency are traversed as not having been shown to be necessarily present. Furthermore, any and all findings of well-known art and Official Notice, or statements interpreted similarly, should not be considered well-known for the particular and specific reasons that the claimed combinations are too complex to support such conclusions and because the Office Action does not include specific findings predicated on sound technical and scientific reasoning to support such conclusions.

If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

Respectfully submitted,

/afb/
Anthony F. Bonner Jr. Reg. No. 55,012

AT&T Legal Department – TKHR
Attn: Patent Docketing
One AT&T Way
Room 2A-207
Bedminster, NJ 07921
Customer No.: **38823**